We claim:

1. A method of transforming an original linear finite state machine circuit including a plurality of memory elements coupled in series and linear logic gates coupled between some of the memory elements, and a feedback connection coupled from a source tap at an output of one of the memory elements to a destination tap coupled to an input of another of the memory elements, comprising:

shifting the source tap of the feedback connection to the right or left along the series of memory elements; and

shifting the destination tap of the feedback connection in a same direction as the source tap to generate a transformed linear finite state machine.

2. The method of claim 1, wherein a majority of memory elements of the transformed linear finite state machine produce an output sequence that is identical to an output sequence of a majority of memory elements of the original linear finite state machine.

3. The method of claim 1, further including determining if the shifted feedback connection caused the source or the destination tap of the feedback connection to cross a source or destination tap of another feedback connection, and if so, adding a new feedback connection.

4. The method of claim 1, wherein the linear finite state machine circuit is a type I LFSR, type II LFSR, or cellular automata.

5. The method of claim 1, wherein the shifting of the source tap is across a same number of memory elements as the shifting of the destination tap.

6. The method of claim 1, wherein shifting the taps of the feedback connection includes reducing the length of the associated feedback connection line.

7. The method of claim 1, wherein shifting the taps of a feedback connection includes reducing the levels of linear logic gates in the original circuit.

8. The method of claim 1, wherein shifting the taps of a feedback connection includes reducing the internal fan-out of the original circuit.

9. The method of claim 1, wherein the linear logic gates are XOR or XNOR gates.

10. A method of transforming an original linear finite state machine, comprising:

providing an original linear finite state machine having multiple memory elements coupled in series with one or more linear logic gates coupled between some of the memory elements;

identifying a feedback connection including a source tap at one end of the feedback connection, the source tap being an output of one of the memory elements, and a destination tap at an opposite end of the feedback connection, the destination tap being an input to one of the memory elements; and

shifting the feedback connection across the memory elements to transform the linear finite state machine.

11. The method of claim 10, wherein the source tap of the original linear finite state machine is coupled to an output of a first memory element and the shifting includes moving the source tap to an output of a second memory element, different than the first memory element.

12. The method of claim 10, wherein shifting includes moving the source and destination taps.

13. The method of claim 10, wherein the linear finite state machine circuit is a type I LFSR, type II LFSR, or cellular automata.

14. The method of claim 10, wherein a computer-readable medium stores instructions thereon for performing the method.

15. The method of claim 10, wherein a majority of memory elements of the transformed linear finite state machine produce an output sequence that is identical to an output sequence of a majority of memory elements of the original linear finite state machine.

16. The method of claim 10, further including determining if the shifted feedback connection caused the source or the destination tap of the feedback connection to cross a source or destination tap of another feedback connection, and if so, adding a new feedback connection.

17. A system of transforming an original linear finite state machine, comprising:

means for identifying a feedback connection in the linear finite state machine; and

means for shifting the feedback connection to transform the linear finite state machine.

18. The system of claim 17, wherein the means for identifying identifies a source tap and a destination tap in the linear finite state machine.

19. The system of claim 18, wherein the means for shifting moves the source tap and the destination tap to different locations than the original finite state machine.